REMARKS

Claims 23-41 are pending. Claims 1-22 were canceled and new claims 23-41 were added.

Request for Interview Prior to Formal Action on Amendment

Applicants requested an interview prior to submission of the enclosed RCE request. In a telephone conversation on February 22, 2005, the Examiner agreed to such an interview after filing of the RCE request. Applicants request such an interview prior to formal action on this amendment. An "Applicant Initiated Interview Request Form" accompanies this RCE request. Please contact Applicants' undersigned representative to schedule the interview.

Prior Art Rejections

Claims 1-22 were rejected under 35 USC 103(a) as allegedly being unpatentable over Messmer in view of different combinations of Newton's Telecom Dictionary, Hill et al. and Kurtzberg et al. This rejection is believed to be moot in view of the cancellation of claims 1-22. The new set of claims are believed to be patentable over these references for at least the reasons discussed below.

1. Messmer

Messmer describes a security monitoring service developed by Counterpane Internet Security. As described in Messmer, a probe is placed on the customer's network to accept audit data from a plurality of network devices. Specifically, a "probe" or "black box" sensor captures syslog and audit outputs from the network devices and transmits the network activity output to Counterpane's data centers where it is monitored around the clock by human analysts. The audit data may have "footprints of attacks" but all that the black box does is to relay them to the data centers where analysts are "trained to understand them." Figure A shows this configuration.

Syslog (i.e., system log) and audit data may or may not contain footprints of an attack. This type of data is routinely collected by many network devices, regardless of whether an attack is occurring on a device.

2. Patentability of claim 23 over Messmer

Counterpane's security system fails to disclose or suggest the claimed combination of a security subsystem and a master system. Counterpane's black box sensor is merely a relaying device which does not, and cannot, detect attacks. Thus, Counterpane's black box sensor cannot be equivalent to the claimed security subsystem which detects attacks on the network. Nor does the data center in Counterpane's security system have any structural elements which detect attacks. Instead, the data center relies upon trained humans to detect attacks. Assuming, *arguendo*, that Counterpane's human-staffed data center is presumed to be equivalent to an entity that detects attacks, then the data center would necessarily have to be equivalent to the claimed security subsystem since that is the claimed element which detects attacks. If so, then Counterpane's security system would lack the claimed master system since nothing in Counterpane's security system monitors the data center and registers information pertaining to attacks detected by the data center, which are the functions performed by the claimed master system.

The Office Action dated August 25, 2004 asserts that Counterpane's black box is the security subsystem and that the data center is the master system, and further asserts the following positions (underlining added for emphasis):

1. "...master system (i.e., Counterpane's data center) registers information pertaining to attacks detected by the security subsystem (i.e., black box)..."

2. "...data that are transmitted to the master system (i.e., data center) are footprints of attacks, and the data center has analysts that are trained to understand them."

As discussed above, the black box does not detect attacks. It is merely a probe that picks up and relays whatever data is in the syslog and audit outputs of the network devices. This data may or may not have any footprints of an attack. That is, the data may be completely clean (i.e., free of attack footprints), or it may be filled with many attack footprints. Nowhere is it described that Counterpane's black box makes any determination of the data contents received by, and

transmitted out of, the black box. This fact is further clarified by the full meaning of the following sentence:

> Embedded in this data are the footprints of attacks, and our analysts are trained to understand them.

As discussed above, syslog and audit data may or may not contain footprints of an attack. This type of data is routinely collected by many network devices, regardless of whether an attack is occurring on a device. Thus, all that the black box does is to pass such data along, regardless of whether or not it contains footprints of an attack. Only the trained analysts perform any attack detection on the data. The two statements highlighted above in the Office Action are thus both incorrect. With respect to the first statement, Counterpane's data center does not register information pertaining to attacks detected by the black box, since the black box performs no such detection. With respect to the second statement, data transmitted to the data center may or may not contain footprints of attacks mixed in with other data, but it is not true that the data transmitted to the data center are footprints of attacks.

In addition, nowhere does Messmer discuss whether the data center can monitor the integrity of the black box. Claim 23 explicitly recites that the master system monitors the integrity of the security subsystem.

In view of the above, claim 23 is believed to be patentable over Messmer.

3. Patentability of claim 23 over Messmer in view of additional applied references

All of the rejections in the Office Action dated August 25, 2004 are based upon the above-discussed mischaracterization of Messmer. The additional references, such as Newton's Telecom Dictionary, Hill et al. and Kurtzberg et al. do not make up for the above-highlighted deficiencies. However, these references are discussed below for completeness.

(i) Newton's Telecom Dictionary

The use of this reference is moot in view of the deletion of the phrase, "secure link" from claim 23.

(ii) Hill et al.

Hill et al. (hereafter, "Hill") discloses a security system that is structurally different from the claimed system. In Hill, a computer network 22 includes a plurality of nodes 24. A computer device 26 and a security agent 36 is located at each node. (The security agent is a software program). The security agents 36 are configured to concurrently detect occurrences of security events 50 on associated nodes 24. Data about security events 50 are collected by the security agents 36 and transmitted to a processor 40. The processor 40 is configured to process security events 50 to form an attack signature. The processor 40 also has the ability to issue instructions to the nodes 24 for mitigating the effects of an attack.

Hill exemplifies one of the deficiencies in many prior art network security systems, namely that the integrity of the very elements that perform network monitoring and attack detection are not monitored. The Office Action dated August 25, 2004 asserts that Hill's security agent 36 is a security subsystem and that Hill's processor 40 is a master system. Applicants strongly disagree with this characterization of Hill. However, assuming, *arguendo*, that Hill can be interpreted against the pending claims in this manner, Hill lacks any disclosure or suggestion that the processor 40 monitors the integrity of any of the security agents 36. Hill just presumes that the security agents 36 are always functioning properly, and if no security events are detected at a particular node 24, then it is presumed that none have occurred. In fact, a security agent 36 at a particular node 24 may have been disabled by an intruder and security events may be occurring at the node 24. For at least this reason, Hill's processor 40 cannot be equivalent to the claimed master system.

(iii) Kurtzberg et al.

Kurtzberg et al. also fails to disclose or suggest the specifically claimed combination of a security subsystem and master system.

In view of the above, claim 23 is believed to be patentable over Messmer, either taken alone, or in combination with any of the other applied references.

4. Patentability of claim 33 over Messmer

Claim 33 is even further removed from Messmer than claim 23. Claim 33 recites:

> (a) a security subsystem associated with at least some of the devices in the network which tests the integrity of the security-related functions;
>
> (b) a master system which monitors the integrity of the security subsystem and receives and stores results of the integrity testing of the devices having security-related functions

Nowhere does Messmer disclose or suggest that either the black box or the data center can "test the integrity" of the security-related functions of any devices in a network. Instead, the "black box" sensor in Messmer merely captures syslog and audit outputs from the network devices and transmits the network activity output to Counterpane's data centers where it is monitored by human analysts.

Furthermore, as discussed above with respect to claim 23, Messmer does not monitor the integrity of the security subsystem.

Messmer thus fails to disclose or suggest at least the above-identified elements of claim 33.

5. Patentability of claim 33 over Messmer in view of additional applied references

All of the rejections in the Office Action dated August 25, 2004 are based upon the above-discussed mischaracterization of Messmer. The additional references, such as Newton's Telecom Dictionary, Hill et al. and Kurtzberg et al. do not make up for the above-highlighted deficiencies with respect to claim 33 for at least the same reasons as discussed above with respect to claim 23.

6. Patentability of dependent claims 24-32 and 34-41

The dependent claims are believed to be patentable over the applied references for at least the reason that they are dependent upon allowable base claims and because they recite additional patentable elements and steps.

Conclusion

Insofar as the Examiner's rejections were fully addressed, the instant application is in condition for allowance. Issuance of a Notice of Allowability of all pending claims is therefore earnestly solicited.

Respectfully submitted,

MICHAEL HRABIK et al.

February 24, 2005 By: Anna Vishev
(Date)

ANNA VISHEV, ESQ.
Registration No. 45,018
SCHULTE ROTH & ZABEL LLP
919 Third Avenue
New York, NY 10022
Telephone: (212) 756-2000
Direct Dial: (212) 756-2167
Facsimile: (212) 593-5955
E-Mail: anna.vishev@srz.com

Enclosure (Figure A)